UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

UNITED STATES OF AMERICA **Plaintiff** **v** **DANIEL MILLS** **Defendant**	1:23-cr-034-LY **INFORMATION** **[Ct. 1: 18 U.S.C. § 1349, Conspiracy to Commit Wire Fraud]**

THE UNITED STATES ATTORNEY CHARGES:

At all times relevant to this Information:

GENERAL ALLEGATIONS

1. DANIEL MILLS resided in Round Rock, Texas. He used the online moniker "Xu" (and variations thereof) and used and controlled the Apple account danielmills0519@gmail.com as well as accounts on the Discord, Instagram, SnapChat, and TikTok platforms.

2. A Subscriber Identity Module ("SIM") card was a technology used to identify and authenticate subscribers on mobile phone devices. It was a chip located inside a mobile phone that stored information identifying and authenticating the subscriber. When a cell phone carrier reassigned a phone number from one physical phone to another—such as when a customer purchased a new phone but wanted to retain the same number—the carrier switched the assignment of the cell phone number from the SIM card in the old phone to the SIM card in the new phone. "SIM swapping" was a term for essentially the same process conducted without the

authorization of the individual who legitimately controlled the phone number. Cybercriminals generally engaged in SIM swapping by convincing a victim's cell phone carrier to reassign the victim's cell phone number from the SIM card inside the victim's cell phone to the SIM card inside a cell phone controlled by the cybercriminals. Cybercriminals may also obtain access to a cell phone carrier's systems and swap victim phone numbers directly.

3. An "account takeover" was a technique that cybercriminals used to take control of a victim's online accounts (*e.g.*, a victim's email, social media, or cryptocurrency accounts) without authorization. Cybercriminals used a variety of techniques to conduct account takeovers. For example, cybercriminals who successfully SIM swapped a victim may then pose as the victim with an online account provider and request that the provider send account password-reset links or an authentication code to the SIM-swapped device now controlled by the cybercriminals. The cybercriminals could then reset the victim's account log-in credentials (*e.g.*, username and password), even if the victim had tried to secure the account by requiring that an authentication code be sent ("two-factor authentication"). Cybercriminals could then use the log-in credentials to access the victim's account without authorization (*i.e.,* "hack into" the account).

4. In a SIM swapping scheme, one or more individuals played the role of the "holder." A holder physically held the SIM card and provided the SIM card number to a co-conspirator with access to the phone carrier's systems. After the phone number was swapped, the holder received the victim's phone calls and text messages. A holder could then complete the account takeover process and access the victim's accounts or pass the victim's credentials to another co-conspirator.

5. Cryptocurrency was an umbrella term for a digital currency in which encryption techniques were used to regulate the generation of units of currency and verify the transfer of funds, generally with relative anonymity. Popular examples of cryptocurrencies included Bitcoin and Ethereum. Users maintained "wallets" and maintained online accounts with cryptocurrency exchanges such as Cryptocurrency Exchange A. Because cryptocurrency wallets were often maintained online, users generally created a phrase or list of words (called a "backup seed") that could be used to recover their online wallets if necessary. The backup seed allowed the user to download the wallet software again and recover the cryptocurrency. However, possession of a backup seed by a cybercriminal would allow the criminal to take control of the online wallet.

6. "Online accounts" included social media accounts and cryptocurrency accounts. "Social Media Platform A" was a social media platform owned by companies based in California which allowed users to share images, video, and text. Users of the platforms were able to send and receive direct messages and follow or be followed by other users. Some users with significant followings, often referred to as "influencers" were able to monetize their social media accounts through techniques such as sponsored links (an advertisement displayed by a search engine when someone searches for keywords), product placements, and product reviews. Companies seeking to advertise their products online frequently paid social media influencers with significant followings to review and promote their products and services. Accounts with significant numbers of followers or with particularly short, unique, or memorable usernames were more highly valued because they were perceived to have a greater income potential.

7. Cybercriminals who engaged in SIM swapping, account takeovers, and cryptocurrency theft often collaborated with one another online, using various online monikers, in forums and on communications platforms like Discord.

8. Cryptocurrency Exchange A was a cryptocurrency exchange based in San Francisco, California with servers located outside the state of Texas.

9. "Victim 1" was a resident of California and an employee of Social Media Platform A.

10. "Victim 2" was a resident of California.

11. "Victim 3" was a resident of Louisiana.

12. "Victim 4" was a resident of Missouri.

13. "Victim 5" was a resident of California.

Object and Purpose of the Conspiracy

14. The object of the conspiracy was to commit wire fraud and obtain things of value from the victims, including, but not limited to, cryptocurrency and control of the victims' social media accounts.

Manner and Means

15. Among the manner and means by which MILLS, together with co-conspirators known and unknown, carried out the conspiracy were the following:

a. Engaging in SIM swapping in order to take control of victims' cell phone numbers.

b. Using their control over the victims' cell phone numbers to perform account takeovers and obtain unauthorized access to the victims' online accounts, including social media accounts and cryptocurrency accounts.

c. Using their access to victims' accounts to take control of and steal things of value from the victims' online accounts, including their account handles and their cryptocurrency.

d. Using victims' hacked online accounts to post unauthorized messages.

e. Communicating with co-conspirators via online social media and chat platforms.

f. Using multiple online accounts and monikers to hide their identities and evade detection by law enforcement.

Overt Acts in Furtherance of the Conspiracy and Acts in Furtherance of the Wire Fraud Scheme

16. On or about August 30, 2019, the cell phone number of Victim 1 was swapped to a phone controlled by MILLS. MILLS was the holder for this SIM swap. On the same day, one or more members of the conspiracy caused password reset information and codes for Victim 1's Social Media Platform A account to be sent via text message to the phone controlled by MILLS. One or more members of the conspiracy accessed Victim 1's Social Media Platform A account without authorization and posted messages, including "nazi Germany did nothing wrong" and "#NIGGER"

17. On or about October 17, 2019, the cell phone number of Victim 2 was swapped to a cell phone controlled by MILLS. MILLS was the holder for this SIM swap. On the same day, MILLS and co-conspirators performed an account takeover and accessed Victim 2's private online accounts and obtained nude photographs of Victim 2 that were then posted on the internet defaced with, among other monikers, MILLS' moniker "Xu."

18. On or about October 25, 2019, the cell phone number of Victim 3 was swapped to a cell phone controlled by MILLS. MILLS was the holder for this SIM swap. On the same day, MILLS and co-conspirators performed an account takeover and accessed Victim 3's private online accounts and obtained nude photographs of Victim 3 that were posted on Victim 3's Instagram page defaced with, among other monikers, MILLS' moniker "Xu."

19. On or about February 1, 2021, the cell phone number of Victim 4 was swapped to a cell phone controlled by MILLS. MILLS was the holder for this SIM swap. MILLS and co-conspirators caused text messages containing two-factor authentication codes for Victim 3's Cryptocurrency Exchange A account to be sent to the cell phone controlled by MILLS. MILLS and co-conspirators performed an account takeover and accessed Victim 3's Cryptocurrency Exchange A account and transferred Bitcoin valued at the time at approximately $124,474.55 at the time to one or more cryptocurrency wallets controlled by MILLS and co-conspirators.

20. On or about February 5, 2021, the cell phone number of Victim 5 was swapped to a cell phone controlled by MILLS. MILLS was the holder for this SIM swap. MILLS and co-conspirators performed an account takeover and accessed Victim 4's Cryptocurrency Exchange A account and transferred Bitcoin valued at the time at approximately $55,482.64 at the time to one or more cryptocurrency wallets controlled by MILLS and co-conspirators.

COUNT ONE
Conspiracy to Commit Fraud
[18 U.S.C. § 1349]

21. Count One incorporates by reference, as if fully set forth herein, paragraphs one through twenty of this Information.

22. On or about August 30, 2019 through February 9, 2021, in the Western District of Texas and elsewhere, the Defendant,

DANIEL MILLS

did knowingly and intentionally conspire and agree with others known and unknown to commit certain offenses against the United States, namely: Wire Fraud, in violation of 18 U.S.C. § 1343, that is, knowingly and with intent to defraud, having devised and having intended to devise a

scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, in this case, engaging in SIM swaps to obtain access to victims' online accounts for the purpose of obtaining things of value from the victims, including, but not limited to, cryptocurrency and control of the victims' social media accounts, and for the purpose of executing the scheme and artifice, transmitted and caused to be transmitted by means of wire, radio and television communication in interstate commerce certain writings, signs, signals, pictures and sounds.

In violation of Title 18, United States Code, Section 1349.

JAIME ESPARZA
UNITED STATES ATTORNEY

By: _____
G. KARTHIK SRINIVASAN
ASSISTANT UNITED STATES ATTORNEY